A Generalization of Grover's Algorithm

Luigi Accardi
Ruben Sabbadini

Centro Vito Volterra
Università degli Studi di Roma "Tor Vergata"
Via Orazio Raimondo, 00173 Roma, Italia
accardi@volterra.mat.uniroma2.it, http://volterra.mat.uniroma2.it

arXiv:quant-ph/0012143v1 27 Dec 2000

ABSTRACT

We investigate the necessary and sufficient conditions in order that a unitary operator can amplify a pre-assigned component relative to a particular basis of a generic vector at the expence of the other components. This leads to a general method which allows, given a vector and one of its components we want to amplify, to choose the optimal unitary operator which realizes that goal. Grover's quantum algorithm is shown to be a particular case of our general method.

However the general structure of the unitary we find is remarkably similar to that of Grover's one: a sign flip of one component combined with a reflection with respect to a vector. In Grover's case this vector is fixed; in our case it depends on a parameter and this allows optimization.

1 Unitary operators which increase the probability of the $|0>$ component of a pre-assigned vector

Let $|i>$ $(i = 0, \ldots, N-1)$ be an orthonormal basis of R^N. The mathematical core of Grover's algorithm is the construction of a unitary operator U which increases the probability of one of the components of a given unit vector,

in the given basis, at the expence of the remaining ones. The necessity of such an amplification of probabilities arises in several problems of quantum computation. For example in the Ohya-Masuda [4] quantum SAT algorithm such a problem arises. In a recent interesting paper Ohya and Volovich have proposed a new method of amplification, based on non linear chaotic dynamics [14]. In the present paper we begin to study the following problem: is it possible to extend Grover's algorithm so that it becomes applicable to a more general class of initial vectors, for example those wich arise in the Ohya-Masuda algorithm? A preliminary step to solve this problem is to determine the most general unitary operator which performs the same task of Grover's operator. This is done in Theorem (1.1) below. The result is rather surprising: we find that, up to the choice of four ± 1 (phases), there exists exactly one class of such unitary operators, labeled by an arbitrary parameter in the interval $[0, 1]$. Moreover these unitaries can be written in a form similar to Grover's one, i.e. a reflection with respect to a given unit vector possibly preceeded by a sign flip of one component combined with, where the unit vector in question depends on this parameter in $[0, 1]$. The free parameter in our problem allows to solve a new problem, which could not be formulated within the framework of Grover's explicit construction, namely the *optimization problem* with respect to the given parameter. We prove that, even in the case of Grover's original algorithm, this additional freedom allows to speed up considerably the amplification procedure. In a forthcoming paper [15] we plan to apply the present method to the Ohya-Masuda algorithm. Since an operator U is unitary if and only if it leaves unaltered the scalar products of vectors with real components in a given basis, we shall restrict our attention to unitary operators with real coefficients in a given basis (as the Grover's ones). This restrictes the problem to R^N.

THEOREM 1 Given the linear functionals:

$$\eta : a = (a_i) \in R^N \mapsto \eta(a) = \sum_{i=0}^{N-1} \eta_i a_i \tag{1}$$

$$c : a = (a_i) \in R^N \mapsto c(a) = \sum_{i=0}^{N-1} \gamma_i a_i \tag{2}$$

with γ_i and η_i real and ε_1, $\varepsilon_2 \in \{\pm 1\}$, necessary and sufficient condition for the operator U, defined by:

$$U \sum a_i |i >= \varepsilon_1 (a_0 + \eta(a))|0 > + \varepsilon_2 \sum_{i \neq 0} (a_i + c(a)) \, |i > \tag{3}$$

to be unitary is that there exist a real number β_0 such that:

$$|\beta_0| \leq 1 \tag{4}$$

$$\gamma_0 \quad = \varepsilon_5 \frac{\sqrt{1 - \beta_0^2}}{\sqrt{N-1}} \tag{5}$$

$$\gamma_i \quad = -\frac{1 + \varepsilon_3 \beta_0}{N-1} \qquad i \neq 0 \tag{6}$$

$$\eta_0 \quad = -1 + \varepsilon_4 \beta_0 \tag{7}$$

$$\eta_i \quad = \varepsilon_3 \gamma_0 \qquad i \neq 0 \tag{8}$$

where ε_3, ε_4, ε_5 are arbitrarily chosen in the set $\{\pm 1\}$.

PROOF In finite dimension unitarity is equivalent to isometry. Therefore U is unitary if and only if, for every $|a >= \sum_{i=0}^{N-1} a_i |i >$ the following isometricy condition is satisfied:

$$\sum a_i^2 = (a_0 + \eta)^2 + \sum_{i \neq 0} (a_i + c)^2 = a_0^2 + \eta^2 + 2a_0 \eta + \sum_{i \neq 0} a_i^2 + (N-1)c^2 + 2c \sum_{i \neq 0} a_i$$

where we write η, c for $\eta(a)$, $c(a)$. This condition can be written in the form:

$$\eta^2 + 2a_0 \eta + (N-1)c^2 + 2c \sum_{i \neq 0} a_i = 0 \tag{9}$$

With the notation:

$$\gamma(a) = \gamma := (N-1)c^2 + 2c \sum_{i \neq 0} a_i \tag{10}$$

Equation (9) is equivalent to:

$$\eta^2 + 2a_0 \eta + \gamma = 0 \tag{11}$$

and its possible solutions are:

$$\eta(a) = \eta = -a_0 + \varepsilon_4 \sqrt{a_0^2 - \gamma(a)} \tag{12}$$

Given (12) the funtional $\eta(a)$ will be linear if and only if $\forall a_0, \ldots, a_N$:

$$a_0^2 - \gamma(a) = \left(\sum_j \beta_j a_j \right)^2 \tag{13}$$

for some real numbers β_j indipendent of a.

Since the functional $c(a)$ is linear and given by (2), because of (12) and (13), condition (9) becomes:

$$-a_0^2 + (N-1) \left(\sum_j \gamma_j a_j \right)^2 + \left(\sum_j \beta_j a_j \right)^2 + 2 \sum_j \gamma_j a_j \sum_{i \neq 0} a_i =$$

$$-a_0^2 + 2 \sum_j \gamma_j a_j \sum_{i \neq 0} a_i + \sum_{i,j} \left[(N-1)\gamma_i \gamma_j + \beta_i \beta_j \right] a_i a_j = 0$$

or equivalently:

$$a_0^2 \left[(N-1)\gamma_0^2 + \beta_0^2 - 1 \right] + \sum_{i,j \neq 0} \left[2\gamma_j + (N-1)\gamma_i \gamma_j + \beta_i \beta_j \right] a_i a_j +$$

$$+ 2 \sum_{i \neq 0} \left[\gamma_0 + (N-1)\gamma_0 \gamma_i + \beta_0 \beta_i \right] a_0 a_i = 0 \tag{14}$$

The identity (14) holds $\forall a_0, \ldots, a_N$, if and only if:

$$(N-1)\gamma_0^2 + \beta_0^2 - 1 = 0 \tag{15}$$

$$2\gamma_j + (N-1)\gamma_i \gamma_j + \beta_i \beta_j = 0 \quad \forall i, j \neq 0 \quad i \neq j \tag{16}$$

$$2\gamma_i + (N-1)\gamma_i^2 + \beta_i^2 = 0 \quad \forall i \neq 0 \tag{17}$$

$$\gamma_0 + (N-1)\gamma_0 \gamma_i + \beta_0 \beta_i = 0 \quad \forall i \neq 0 \tag{18}$$

Equation (15) and the reality condition on η imply that (4) and (5) hold. From (18) we deduce that, for $i \neq 0$:

$$\gamma_i = -\frac{\gamma_0 + \beta_0 \beta_i}{\gamma_0 (N-1)} \tag{19}$$

and, replacing this into (17), we find:

$$-\frac{2(\gamma_0+\beta_0\beta_i)}{\gamma_0(N-1)}+\frac{(\gamma_0+\beta_0\beta_i)^2}{\gamma_0^2(N-1)}+\beta_i^2=0$$

or:

$$\left[(N-1)\,\gamma_0^2+\beta_0^2\right]\beta_i^2=\gamma_0^2$$

which, because of (15), is equivalent to:

$$\beta_i=\varepsilon_3\gamma_0=\varepsilon_3\varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} \tag{20}$$

with $\varepsilon_3=\pm 1$. Replacing (20) into (19) we arrive to (6)

Replacing (24),..., (27) into (1) and (2), we conclude that a necessary condition for the linearity of U is that η and c must have the form:

$$\eta(a)=(-1+\varepsilon_4\beta_0)a_0+\varepsilon_4\varepsilon_3\gamma_0\sum_{k\neq 0}a_k=(-1+\varepsilon_4\beta_0)a_0+\varepsilon_4\varepsilon_3\varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}}\sum_{k\neq 0}a_k \tag{21}$$

$$c(a)=\gamma_0a_0-\frac{1+\varepsilon_3\beta_0}{N-1}\sum_{k\neq 0}a_k=\varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}}a_0-\frac{1+\varepsilon_3\beta_0}{N-1}\sum_{k\neq 0}a_k \tag{22}$$

Conversely, if conditions (4), ..., (8) are satisfied, then also (14), which is equivalent to (9), is satisfied and therefore U is isometric, hence unitary. This can also be seen by a direct computation (see appendix A).

REMARK Because of (4) there exists a $\theta\in[0,2\pi)$ such that β_0 has the form:

$$\beta_0=\varepsilon_3 cos\ \theta \tag{23}$$

and therefore, from (5):

$$\sqrt{N-1}\gamma_0=\varepsilon_5\sqrt{1-\beta_0^2}=sin\ \theta \tag{24}$$

i.e. the parameters β_0 and γ_0 live onto an ellipse in the $(\beta_0,\ \gamma_0)$-plane. With these notations one has:

$$\eta(a)=(-1+\varepsilon_3\varepsilon_4 cos\ \theta)\,a_0+\varepsilon_3\varepsilon_4\frac{sin\ \theta}{\sqrt{N-1}}\sum_{k\neq 0}a_k \tag{25}$$

$$c(a) = \frac{sin\ \theta}{\sqrt{N-1}} a_0 - \frac{1 + cos\ \theta}{N-1} \sum_{k \neq 0} a_k \tag{26}$$

REMARK The case $\gamma = 0$ leads to $\eta = 0$ or $\eta = -2a_0$; in both cases we have:

$$U \sum a_i |i >= \pm\varepsilon_1 a_0\ |0 > +\varepsilon_2 \sum_{i \neq 0} (a_i + c)\ |i >$$

The operators $U(\gamma \equiv 0(a))$ are in this class, however they play a significant role in Grover's algorithm because they may be used to change the sign of a component leaving the others u inaltered (*flip*).

If we are interested in unitaries which modify the component a_0 of a, we must look for solutions with $\gamma \neq 0$.

COROLLARY 2 If in (21) and (22) we choose:

$$\varepsilon_1 \varepsilon_4 = \varepsilon_3 = \varepsilon_5 = 1$$
$$\varepsilon_2 = -1$$
$$\beta_0 = \frac{N-2}{N}$$
$$\gamma_0 = \frac{2}{N}$$

then the corresponding operator U is Grover's unitary (see section 4).

PROOF It is known that Grover's unitary is characterized by (see section 4):

$$a_0 \mapsto \frac{N-2}{N} a_0 + \frac{2}{N} \sum_{k \neq 0} a_k =: \varepsilon_1 [a_0 + \eta(a)] \tag{27}$$

$$a_i \mapsto -a_i + \frac{2}{N} \left(-a_0 + \sum_{k \neq 0} a_k \right) =: \varepsilon_2 [a_i + c(a)] \tag{28}$$

On the other hand, from equations (25) and (26) we have:

$$\varepsilon_1 [a_0 + \eta(a)] = \varepsilon_1 \varepsilon_4 \left(\beta_0 a_0 + \varepsilon_3 \gamma_0 \sum_{k \neq 0} a_k \right) \tag{29}$$

$$\varepsilon_2 \left[a_i + c(a)\right] = \varepsilon_2 \left(a_i + \gamma_0 a_0 - \frac{1 + \varepsilon_3 \beta_0}{N-1} \sum_{k \neq 0} a_k \right) \tag{30}$$

with γ_0 given by (5). Comparing this with (27) and (28) we see that the condition for equality is:

$$\varepsilon_1 \varepsilon_4 \beta_0 = \frac{N-2}{N}$$

Now let us choose $\varepsilon_1 \varepsilon_4 = 1$ and $\beta_0 = \frac{N-2}{N}$ then:

$$\gamma_0 = \varepsilon_5 \sqrt{\frac{1 - \frac{(N-2)^2}{N^2}}{N-1}} = \varepsilon_5 \frac{2}{N}$$

that leads to $\varepsilon_5 = 1$. Therefore, if $\varepsilon_2 = -1$, the coefficient of the third term in (30) becomes:

$$-\varepsilon_2 \frac{1 + \varepsilon_3 \beta_0}{N-1} = \frac{1 + \varepsilon_3 \frac{N-2}{N}}{N-1} = \frac{N + \varepsilon_3 N - 2\varepsilon_3}{N(N-1)}$$

that gives the correct parameter $\frac{2}{N}$ if and only if $\varepsilon_3 = 1$.

2 Canonical form and reflections

THEOREM 1 Any unitary operator $U(\beta_0, \varepsilon)$ with real coefficients in the basis $(|i>)$ and satisfying the conditions of Theorem (1.1), can be written in the form:

$$U(\beta_0, \varepsilon) := \varepsilon_1 \varepsilon_4 |0> \left(\beta_0 \ <0| + \varepsilon_3 \varepsilon_5 \frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} \sum_{k \neq 0} <k| \right) +$$

$$+ \varepsilon_2 \sum_{i \neq 0} |i> \ \left(<i| + \varepsilon_5 \frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} <0| - \frac{1 + \varepsilon_3 \beta_0}{N-1} \ \sum_{k \neq 0} <k| \right) \tag{31}$$

Moreover a unit vector $u \in R^N$ such that:

$$U(\beta_0, \varepsilon) = \varepsilon_2 \left(1 - 2|u><u|\right) \tag{32}$$

exists if and only if ε is such that

$$\varepsilon_2 = \varepsilon_1 \varepsilon_4 \varepsilon_3 \tag{33}$$

In this case $|u>$ has the form:

$$|u>= \frac{1}{\sqrt{2}} \left| -\varepsilon_5 \sqrt{1-\varepsilon_3 \beta_0},\ \sqrt{\frac{1+\varepsilon_3\beta_0}{N-1}},\ \ldots,\ \sqrt{\frac{1+\varepsilon_3\beta_0}{N-1}} \right\rangle \tag{34}$$

REMARK Notice that unitary operator (32) simply realizes the reflection of the $|u>$-component of any vector with respect to the $|u>$-axis.
PROOF The identity (31) follows immediately from (2), (21) and (22).

The operator $U(\beta_0, \varepsilon)$ of the equation (31) can be rapresented in the following way:

$$U(\beta_0,\varepsilon) := \varepsilon_2 1 - \left\{ |0> \left[(\varepsilon_2 1 - \varepsilon_1\varepsilon_4\beta_0) < 0| - \varepsilon_1\varepsilon_4\varepsilon_3\varepsilon_5 \frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} \sum_{k\neq 0} < k| \right] + \right.$$

$$\left. + \varepsilon_2 \sum_{i\neq 0} |i> \left(-\varepsilon_5 \frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} < 0| + \frac{1+\varepsilon_3\beta_0}{N-1} \sum_{k\neq 0} < k| \right) \right\} \tag{35}$$

Now an easy calculation shows that, given a vector $|u>$ of the form (35), the right end side of (32) is equal to:

$$\varepsilon_2 1 - \left\{ |0> \left[\varepsilon_2 (1-\varepsilon_3\beta_0) < 0| - \varepsilon_2\varepsilon_5 \frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} \sum_{k\neq 0} < k| \right] + \right.$$

$$\left. + \varepsilon_2 \sum_{i\neq 0} |i> \left((-\varepsilon_5 \frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} < 0| + \frac{1+\varepsilon_3\beta_0}{N-1} \sum_{k\neq 0} < k| \right) \right\} \tag{36}$$

For $\beta_0 \neq 0, 1$ (36) and (35) are equal if and only if (33) holds. and the last operator is a projector if and only if:

$$\varepsilon_2 = \varepsilon_1 \varepsilon_4 \varepsilon_3 \tag{37}$$

because the off-diagonal terms must be equal. From this the thesis follows observing that multiplying (37) for $\varepsilon_2\varepsilon_3$ we obtain:

$$\varepsilon_3 = \varepsilon_1 \varepsilon_4 \varepsilon_2 \tag{38}$$

COROLLARY 2 Grover's operator is the product of a operator of the form (32) with a *flip*, realized with a operator $U(\gamma = 0, \ \forall a)$, as in the Remark after previous Theorem 2.1.

PROOF As it is implicit in its definition (see Section 4), Grover's operator is a *flip* followed by a reflection of the $|v>$-component with respect to the $|v>$-axis, where $|v>:= N^{-1/2}|1,\ldots,1>$.

REMARK Theorem (2.1) shows that Grover's unitary and the generalized ones presented in this paper are analogue, and the realizability of the former implies the realizability of the latter.
REMARK If in (35) the identity (37) holds then, remembering (23) and (24), we can rewrite (35) inthe form:

$$|u>= \left| -\sin\frac{\theta}{2}, \ \frac{\cos\frac{\theta}{2}}{\sqrt{N-1}}, \ \ldots, \ \frac{\cos\frac{\theta}{2}}{\sqrt{N-1}} \right\rangle \tag{39}$$

which, up to a phase, is the most general form of a vector in R^N with $N-1$ components equal.

REMARK A matrix rapresentation of the operator $U(\beta_0, \varepsilon)$ in the basis $(|i>)$, with $\varepsilon_2 = \varepsilon_1\varepsilon_4\varepsilon_3$ is:

$$U(\beta_0,\varepsilon) = \varepsilon_2 \begin{pmatrix} 1+\varepsilon_3\beta_0 - 1 & \varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} & \varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} & \ldots & \varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} \\ \varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} & 1-\frac{1+\varepsilon_3\beta_0}{N-1} & -\frac{1+\varepsilon_3\beta_0}{N-1} & \ldots & -\frac{1+\varepsilon_3\beta_0}{N-1} \\ \varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} & -\frac{1+\varepsilon_3\beta_0}{N-1} & 1-\frac{1+\varepsilon_3\beta_0}{N-1} & \ldots & -\frac{1+\varepsilon_3\beta_0}{N-1} \\ \vdots & \vdots & & \ddots & \\ \varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} & -\frac{1+\varepsilon_3\beta_0}{N-1} & -\frac{1+\varepsilon_3\beta_0}{N-1} & \ldots & 1-\frac{1+\varepsilon_3\beta_0}{N-1} \end{pmatrix} =$$

$$= \varepsilon_2 1 - \varepsilon_2 \begin{pmatrix} 1-\varepsilon_3\beta_0 & -\varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} & \ldots & -\varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} \\ -\varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} & \frac{1+\varepsilon_3\beta_0}{N-1} & \ldots & \frac{1+\varepsilon_3\beta_0}{N-1} \\ \vdots & \vdots & \ddots & \vdots \\ -\varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} & \frac{1+\varepsilon_3\beta_0}{N-1} & \ldots & \frac{1+\varepsilon_3\beta_0}{N-1} \end{pmatrix} =$$

$$= \varepsilon_2 1 - \varepsilon_2 \begin{pmatrix} 1 - cos\ \theta & -\frac{sin\ \theta}{\sqrt{N-1}} & \dots & -\frac{sin\ \theta}{\sqrt{N-1}} \\ -\frac{sin\ \theta}{\sqrt{N-1}} & \frac{1+cos\ \theta}{N-1} & \dots & \frac{1+cos\ \theta}{N-1} \\ \vdots & \vdots & \ddots & \vdots \\ -\frac{sin\ \theta}{\sqrt{N-1}} & \frac{1+cos\ \theta}{N-1} & \dots & \frac{1+cos\ \theta}{N-1} \end{pmatrix} =$$

$$= \varepsilon_2 1 - \varepsilon_2 2 \begin{pmatrix} sin^2\ \frac{\theta}{2} & -\frac{sin\ \frac{\theta}{2} cos\frac{\theta}{2}}{\sqrt{N-1}} & \dots & -\frac{sin\ \frac{\theta}{2} cos\frac{\theta}{2}}{\sqrt{N-1}} \\ -\frac{sin\ \frac{\theta}{2} cos\frac{\theta}{2}}{\sqrt{N-1}} & \frac{cos^2\ \frac{\theta}{2}}{N-1} & \dots & \frac{cos\frac{\theta}{2}}{N-1} \\ \vdots & \vdots & \ddots & \vdots \\ -\frac{sin\ \theta}{\sqrt{N-1}} & \frac{cos\ \frac{\theta}{2}}{N-1} & \dots & \frac{cos^2\ \frac{\theta}{2}}{N-1} \end{pmatrix} =$$

$$= \varepsilon_2 \left(1 - 2|u >< u|\right) \tag{40}$$

with $|u>$ given by (35) or (39).

3 Optimal Choice of the Parameters

In this section we study the following generalization of Grover's problem: given a fixed vector $|a >= \sum_i a_i |i>$, we look for a unitary operator $U = U(\beta_0, \varepsilon)$ of the form discussed in sections (1) and (2), which increases the probability of the 0-th component of $|a>$, i.e. such that:

$$|a_0| < |(U(\beta_0, \varepsilon)|a>)_0| := |< 0|U(\beta_0, \varepsilon)|a>| \tag{41}$$

DEFINITION 1 A unitary operator $U(\beta_0, \varepsilon)$ of the form discussed in sections (1) and (2) is an *optimal amplifier* for the 0-th component of $|a>$ if condition (41) is satisfied and:

$$|(U(\beta_0, \varepsilon)|a>)_0| \leq |(U(\overline{\beta}_0, \overline{\varepsilon})|a>)_0| \tag{42}$$

$\forall \beta_0 \in [0,1]\,;\ \forall \varepsilon := (\varepsilon_1,\ \dots,\ \varepsilon_5) \in \{\pm 1\}^5$. If moreover:

$$|(U(\overline{\beta}_0, \overline{\varepsilon})|a>)_0| = 1 \tag{43}$$

then we speek of an *absolute optimal amplifier*.

THEOREM 2 Given a unit vector of the form:

$$|a_G>:= a_0|0> +b\sum_{i\neq 0}|i> \tag{44}$$

with $a_0 \neq 0$ and

$$a_0^2 + (N-1)b^2 = 1; \tag{45}$$

an absolute optimal amplifier exists and is defined by: $\beta_0 = \pm a_0$.
PROOF From equations (21), (22), (25) and (26) we have:

$$U|a_G>:= U\left(a_0|0> +b\sum_{i\neq 0}|i>\right) =$$

$$= \varepsilon_1\varepsilon_4\left[\beta_0 a_0 + \varepsilon_3\varepsilon_5\sqrt{(N-1)(1-\beta_0^2)}b\right]|0> +$$

$$+\varepsilon_2\left[b + \varepsilon_5\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}}a_0 - (1+\varepsilon_3\beta_0)\,b\right]\sum_{i\neq 0}|i>=$$

$$= \varepsilon_1\varepsilon_4\varepsilon_3\left(cos\ \theta a_0 + \sqrt{N-1}sen\ \theta\ b\right)|0> +\varepsilon_2\left(\frac{sen\ \theta}{\sqrt{N-1}}a_0 - cos\ \theta\ b\right)\sum_{i\neq 0}|i>$$

The amplitude of $|0>$ is extremal if:

$$\frac{\partial}{\partial\ \theta}\left(cos\ \theta a_0 + \sqrt{N-1}sen\ \theta\ b\right) = -sen\ \theta\ a_0 + \sqrt{N-1}cos\ \theta\ b = 0$$

and this is satisfied by a $\overline{\theta}$ such that:

$$tg\ \overline{\theta}\ = \sqrt{N-1}\frac{b}{a_0} \tag{46}$$

that gives:

$$\varepsilon_3\beta_0 = cos\ \overline{\theta} = \frac{\varepsilon_6}{\sqrt{1+tg^2\ \overline{\theta}}} = \varepsilon_6 a_0$$

and

$$\varepsilon_5\sqrt{1-\beta_0^2} = sin\ \overline{\theta} = \frac{\varepsilon_7 tg\ \overline{\theta}}{\sqrt{1+tg^2\ \overline{\theta}}} = \varepsilon_7\sqrt{N-1}b$$

where $\varepsilon_6, \varepsilon_7 \in \{\pm 1\}$ and we used (45). From (46) we have $\varepsilon_6 = \varepsilon_7$.

Therefore we obtain:

$$a_0 \mapsto \varepsilon_1\varepsilon_4\varepsilon_3\varepsilon_6 \left(sen^2\ \overline{\theta} + cos^2\ \overline{\theta} \right) = \varepsilon_1\varepsilon_4\varepsilon_3\varepsilon_6$$

and

$$b \mapsto \varepsilon_2\varepsilon_6 \left(\frac{sen\ \overline{\theta} cos\ \overline{\theta}}{\sqrt{N-1}} - \frac{sen\ \overline{\theta} cos\ \overline{\theta}}{\sqrt{N-1}} \right) = 0$$

Thus the extremal amplitudes correspond to probability 1 and this completes the proof.

REMARK The absolute optimality of the previous Theorem (3.2) refers to the case when all the components $a_k (k \neq 0)$ are equal. However, for a general vector, an optimal amplifier will not be absolutely optimal. This fact will be apparent from the following theorem.

THEOREM 3 An optimal amplifier for a generic vector a of the form:

$$|a> := \sum_{j=0}^{N} a_j |j> \tag{47}$$

with:

$$\sum_j a_j^2 = 1 \tag{48}$$

exists if $\sum_{k\neq 0} a_k \neq 0$ and it is given by an operator (31) with the following choice: $tg\ \theta = \frac{\sum_{k\neq 0} a_k}{a_0\sqrt{N-1}}$.

PROOF From equations (21), (22), (25) and (26) we have:

$$U|a> := U \sum_{j=0}^{N} a_j |j> = \varepsilon_1\varepsilon_4 \left(\beta_0 a_0 + \varepsilon_3\varepsilon_5 \frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} \sum_{k\neq 0} a_k \right) |0> +$$

$$+\varepsilon_2 \sum_{i\neq 0} \left(a_i + \varepsilon_5 \frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} a_0 - \frac{1+\varepsilon_3\beta_0}{N-1} \sum_{k\neq 0} a_k \right) |i> =$$

$$= \varepsilon_1\varepsilon_4\varepsilon_3 \left(cos\ \theta a_0 + \frac{sen\ \theta}{\sqrt{N-1}} \sum_{k\neq 0} a_k \right) |0> +$$

$$+\varepsilon_2 \sum_{i\neq 0}\left(a_i + \frac{sen\ \theta}{\sqrt{N-1}}a_0 - \frac{1+cos\ \theta}{N-1}\sum_{k\neq 0} a_k\right)|i>=$$

and the amplitude of $|0>$ is extremal for:

$$\frac{\partial}{\partial\ \theta}\left(cos\ \theta a_0 + \frac{sen\ \theta}{\sqrt{N-1}}\sum_{k\neq 0} a_k\right) = -sen\ \theta a_0 + \frac{cos\ \theta}{\sqrt{N-1}}\sum_{k\neq 0} a_k = 0$$

then for a $\overline{\theta}$ such that:

$$tg\ \overline{\theta}\ = \frac{\sum_{k\neq 0} a_k}{a_0\sqrt{N-1}}$$

this gives:

$$\varepsilon_3\beta_0 = cos\ \overline{\theta}\ = \frac{\varepsilon_6}{\sqrt{1+tg^2\ \overline{\theta}}} = \frac{\varepsilon_6}{\sqrt{1+\frac{(\sum_{k\neq 0} a_k)^2}{a_0^2(N-1)}}} = \frac{\varepsilon_6 a_0\sqrt{N-1}}{\sqrt{a_0^2(N-1)+(\sum_{k\neq 0} a_k)^2}}$$

$$\sqrt{N-1}\gamma_0 = sen\ \overline{\theta} = \frac{\varepsilon_7 tg\ \overline{\theta}}{\sqrt{1+tg^2\ \overline{\theta}}} = \frac{\varepsilon_7\sum_{k\neq 0} a_k}{\sqrt{a_0^2(N-1)+(\sum_{k\neq 0} a_k)^2}}$$

with ε_6, $\varepsilon_7 \in \pm 1$ and $\varepsilon_6\varepsilon_7 = 1$, i.e. $\varepsilon_6 = \varepsilon_7$. This gives:

$$a_0 \mapsto \frac{\varepsilon_1\varepsilon_4\varepsilon_3\varepsilon_6\left[a_0^2(N-1)+(\sum_{k\neq 0} a_k)^2\right]}{\sqrt{N-1}\sqrt{a_0^2(N-1)+(\sum_{k\neq 0} a_k)^2}} =$$

$$= \frac{\varepsilon_1\varepsilon_4\varepsilon_3\varepsilon_6\sqrt{a_0^2(N-1)+(\sum_{k\neq 0} a_k)^2}}{\sqrt{N-1}} = \varepsilon_1\varepsilon_4\varepsilon_3\varepsilon_6\sqrt{a_0^2+\frac{\left(\sum_{k\neq 0} a_k\right)^2}{N-1}} \quad (49)$$

Finally:

$$a_i \mapsto \varepsilon_2\left[a_i + \frac{\varepsilon_6}{\sqrt{N-1}}\frac{\sum_{k\neq 0} a_k}{\sqrt{a_0^2(N-1)+(\sum_{k\neq 0} a_k)^2}}a_0 - \frac{1+\varepsilon_6\frac{a_0\sqrt{N-1}}{\sqrt{a_0^2(N-1)+(\sum_{k\neq 0} a_k)^2}}}{N-1}\sum_{k\neq 0} a_k\right] =$$

$$= \varepsilon_2\left(a_i - \frac{\sum_{k\neq 0} a_k}{N-1}\right) \quad (50)$$

and this completes the proof.

REMARK Obviously (49) and (50) shall be as in Theorem (3.2) if the vector $|a>$ is of the form (44).
REMARK The action of the *optimal amplifier* found in Theorem (3.3) can be described in the following way: "For every $|a>$:

1. we subtract from every a_i, $i \neq 0$, the average of all the components different from the 0-th one:

$$a_i \mapsto a_i - \frac{\sum_{k\neq 0} a_k}{N-1}$$

2. Then for the 0's component we have of course:

$$a_0 \mapsto \sqrt{1 - \sum_{i\neq 0}\left(a_i - \frac{\sum_{k\neq 0} a_k}{N-1}\right)^2} =$$

$$= \sqrt{1 - \sum_{i\neq 0} a_i^2 - (N-1)\frac{\left(\sum_{k\neq 0} a_k\right)^2}{(N-1)^2} + 2\frac{\left(\sum_{i\neq 0} a_i\right)\left(\sum_{k\neq 0} a_k\right)}{N-1}} =$$

$$= \sqrt{a_0^2 + \frac{\left(\sum_{k\neq 0} a_k\right)^2}{N-1}}$$

(where in the last step we used (48)) as in the (49)".

4 Grover's algorithm

Grover, in [1], considers the following problem (cf also [2]):
PROBLEM: Given a (quantum) system with a state space $\mathcal{H}$ of dimension $N = 2^n$. Let $\{0,1\}^N = \{S_0, S_2, \ldots, S_{N-1}\} =: S$ be the set of states represented as n q-bit string $\in \mathcal{H}$. Let be given a function:

$$C : S \mapsto \{0, 1\}$$

with the following property: there is only one state, say S_v, such that $C(S_v) = 1$, while $C(S) = 0 \quad \forall S \neq S_v$. Construct a quantum computer algorithm which is able to find the unknown S_v state with high (say $> .5$) probability.

It is always possible to rename the states so that $\{S_1, \ldots, S_N\} = \{0, \ldots, N-1\}$ and $S_v = 0$. In these notations let be given a vector:

$$|a> := \sum_i a_i |i>$$

The first step in Grover's algorithm is to construct an operator Z that *flips* the 0-component. In our notations:

$$Z := 1 - 2|0><0|$$

Grover then defines:

$$|\tilde{a}> := Z|a> = -a_0|0> + \sum_{i\neq 0} a_i|i>$$

and chooses the unit vector in formula (32) as follows:

$$|v> := \frac{1}{\sqrt{N}} \sum_k |k> = \frac{1}{\sqrt{N}} |1, \ldots, 1> \tag{51}$$

This gives:

$$<v|\tilde{a}> = \frac{1}{\sqrt{N}} \sum_k <k| \left(-a_0|0> + \sum_{i\neq 0} a_i|i> \right) = \frac{1}{\sqrt{N}} \left(-a_0 + \sum_{k\neq 0} a_k \right)$$

Then, denoting $P := |v><v|$, Grover introduces the unitary operator $D|\tilde{a}> := -1 + 2P$, whose action on $|\tilde{a}>$ is given by:

$$D|\tilde{a}> := (-1+2P)\,|\tilde{a}> = -|\tilde{a}> + 2<v|\tilde{a}>\ |v> = -|\tilde{a}> + \frac{2}{\sqrt{N}} \left(-a_0 + \sum_{k\neq 0} a_k \right)\ |v>$$

$$= \left[\left(1 - \frac{2}{N} \right) a_0 + \frac{2}{N} \sum_{k\neq 0} a_k \right] |0> + \sum_{i\neq 0} \left[-a_i + \frac{2}{N} \left(-a_0 + \sum_{k\neq 0} a_k \right) \right]\ |i>$$

Then:

$$a_0 \mapsto \frac{N-2}{N} a_0 + \frac{2}{N} \sum_{k\neq 0} a_k = \varepsilon_1 \left[a_0 + \eta(a) \right] \tag{52}$$

$$a_i \mapsto -a_i + \frac{2}{N}\left(-a_0 + \sum_{k\neq 0} a_k\right) = \varepsilon_2\left[a_i + c(a)\right] \tag{53}$$

If $a_k = a_h \ \ \forall k,\ h \neq 0$ (the Grover's agorithm case) then:

$$a_0 \mapsto \frac{N-2}{N}a_0 + \frac{2(N-1)}{N}a_i$$

$$a_i \mapsto \left[-1 + \frac{2(N-1)}{N}\right]a_i - \frac{2}{N}a_0$$

We can arrive to the same result working only *via* operator algebra. Grover's unitary is therefore:

$$U_G := DZ = -(1 - 2|v >< v|)(1 - 2|0 >< 0|) =$$

$$= -1 + 2|v >< v| + 2|0 >< 0| - \frac{4}{\sqrt{N}})|v >< 0|$$

and it acts on $|a>$ in the following way:

$$(-1 + 2|v >< v| + 2|0 >< 0| - \frac{4}{\sqrt{N}})|v >< 0|)|a >=$$

$$= \left| a_0 + \frac{2}{N}\sum_{j=0}^{N-1} a_j - \frac{4}{N}a_0,\ \left(a_i + \frac{2}{N}\sum_{j=0}^{N-1} a_j - \frac{4}{N}a_0\right)_{i=1,\dots,N-1}\right\rangle =$$

$$= \left|\left(1 - \frac{2}{N}\right)a_0 + \frac{2}{N}\sum_{k\neq 0} a_k,\ \left(\frac{2}{N}a_0 - a_i + \frac{2}{N}\sum_{k\neq 0} a_k\right)_{i=1,\dots,N-1}\right\rangle \tag{54}$$

Comparing (54) with (49)and (50) we conclude that, within the class $U(\beta_0, \varepsilon)$, Grover's unitary is not optimal, not only for a generic initial vector $|a>$, but even for the initial vector $|a_G>$ used by Grover himself and given by (45).

5 A One Step Solution for Grover's Problem

In the notations of section (4) let us write $|j>$ for the state S_j so that, in particular, $|S_v>=|v>$, and suppose moreover that $j = 0, 1, \dots, N-1$.

In Grover's algorithm one uses the unitary operator:

$$V|j>=(-1)^{C(S_j)}|j>$$

which is a self adjoint involution, i.e. $V = V^*$ and $V^2 = 1$

We will consider the unitary operator:

$$V|j>=\begin{cases} |j> & if\ j \neq 0\ or\ C(S_j)=0 \\ |0> & if\ C(S_j)=1 \\ |j> & if\ j=0\ and\ C(S_v)=1 \end{cases}$$

which is also an involution ($V^2 = 1$).

Notice that $V|j>=\sum_k u_{jk}|k>$ and $u_{jk} = \delta_{jk}$ if $j \neq v, 0$; $u_{vo} = 1$, $u_{vk} = 0$ for $k \neq v$, $u_{0v} = 1$, $u_{0k} = 0$ for $k \neq v$. Thus V is a local operator in the sense of Grover [1], section (5). The action of V can be compactly described by:

$$V|j>=(1-\delta_{1,C(S_0)})\delta_{0,C(S_j)}|j>+\delta_{1,C(S_j)}|0>+(1-\delta_{1,C(S_0)})\delta_{j,0}+$$
$$+\frac{1}{2}\sum_{k=1}\left[1-(-1)^{C(S_k)}\right]|k> \tag{55}$$

from which it is clear that the physical action of V is realized by parallel computation of the values of C, exactly as in Grover's algorithm.

THEOREM In Theorem (3.2) let us choose the initial vector $|a_G>$ in (45) so that $a_0 = b = \frac{1}{\sqrt{N}}$ (i.e. we choose Grover's initial vector) and let us denote U the corresponding absolute uptimal unitary operator. Define:

$$U_{OPT} := V^*UV$$

then U_{OPT} is an absolute optimal amplifier for the component $|S_v>$ of $|a_G>$.
PROOF Clear from theorem (3.2) and the definition of U.

6 APPENDIX A: Direct proof that U verifies the Isometricity Condition

Let us now verify that the set of conditions (4), …, (8) are also sufficient conditions. To this goal we check if the isometricity condition (11) is satisfied by the operator U, given by (3) if the parameters satisfy (4), …, (8). Then, replacing (21) and (22), which are equivalent to (4), …, (8), into (10) and the (12), we find:

$$\eta(a)^2 = (-1+\varepsilon_4\beta_0)^2 a_0^2 + \frac{1-\beta_0^2}{N-1}\left(\sum_{k\neq 0} a_k\right)^2 + 2\varepsilon_4\varepsilon_3\varepsilon_5 a_0(-1+\varepsilon_4\beta_0)\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}}\sum_{k\neq 0} a_k$$

$$2a_0\eta(a) = 2(-1+\varepsilon_4\beta_0)a_0^2 + 2\varepsilon_4\varepsilon_3\varepsilon_5 a_0\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}}\sum_{k\neq 0} a_k$$

$$\eta(a)^2 + 2a_0\eta(a) = (-1+\beta_0^2)a_0^2 + \frac{1-\beta_0^2}{N-1}\left(\sum_{k\neq 0} a_k\right)^2 + 2\varepsilon_3\varepsilon_5 a_0\beta_0\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}}\sum_{k\neq 0} a_k$$

$$(N-1)c(a)^2 = (1-\beta_0^2)a_0^2 + \frac{(1+\varepsilon_3\beta_0)^2}{(N-1)^2}\left(\sum_{k\neq 0} a_k\right)^2 - 2\varepsilon_5 a_0\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}}(1+\varepsilon_3\beta_0)\sum_{k\neq 0} a_k$$

$$2c(a)\sum_{k\neq 0} a_k = 2\varepsilon_5 a_0\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}}\sum_{k\neq 0} a_k - 2\frac{1+\varepsilon_3\beta_0}{N-1}\left(\sum_{k\neq 0} a_k\right)^2$$

Therefore the isometricity condition (11) is equivalent to:

$$\eta(a)^2 + 2a_0\eta(a) = (\beta_0^2-1)a_0^2 + \frac{1-\beta_0^2}{N-1}\left(\sum_{k\neq 0} a_k\right)^2 + 2\varepsilon_3\varepsilon_5 a_0\beta_0\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}}\sum_{k\neq 0} a_k =$$

$$= -\gamma = (-1+\beta_0^2)a_0^2 - \frac{(1+\varepsilon_3\beta_0)^2}{(N-1)^2}\left(\sum_{k\neq 0} a_k\right)^2 + 2\varepsilon_5 a_0\frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}}(1+\varepsilon_3\beta_0)\sum_{k\neq 0} a_k +$$

$$-2\varepsilon_5 a_0 \frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} \sum_{k\neq 0} a_k + 2\frac{1+\varepsilon_3\beta_0}{N-1^2}\left(\sum_{k\neq 0} a_k\right)^2$$

or equivalently:

$$(\beta_0^2-1)a_0^2 + \frac{1-\beta_0^2}{N-1}\left(\sum_{k\neq 0} a_k\right)^2 + 2\varepsilon_3\varepsilon_5 a_0\beta_0 \frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}} \sum_{k\neq 0} a_k =$$

$$= (-1+\beta_0^2)a_0^2 + \frac{2(1+\varepsilon_3\beta_0)-(1+\varepsilon_3\beta_0)^2}{(N-1)^2}\left(\sum_{k\neq 0} a_k\right)^2 +$$

$$+2\varepsilon_5 a_0 \frac{\sqrt{1-\beta_0^2}}{\sqrt{N-1}}(1+\varepsilon_3\beta_0-1)\sum_{k\neq 0} a_k$$

which is an identity for any choice of ε_3, ε_4, ε_5 and this ends the proof.

7 Bibliography

[1] Lov K. Grover: Quantum Mechanics helps in searching for a needle in a haystack, Phys. Rev. Lett. 79, 325-328

[2] Boyer M, Brassard G, Hoyer P and Tapp A: Tight bounds on quantum searching (preprint quant-ph/9605034)

[3] Luigi Accardi, Ruben Sabbadini: On the Ohya–Masuda quantum SAT algorithm Volterra preprint 2000,

[4] M. Ohya and N. Masuda, *NP problem in Quantum Algorithm*, quant–ph/9809075.

[5] M. Ohya, *Mathematical Foundation of Quantum Computer*, Maruzen Publ. Company, 1998.

[6] A. Yu. Kitaev: Quantum measurement and the abelian stabilizer problem, quant-ph/9511026, 20-11 (1995)

[7] M. Ohya, N. Watanabe: On Mathematical treatment of Fredkin-Toffoli-Milburn gate, Physica D, 120 (1998) 206-213

[8] I.V. Volovich, Quantum Computers and Neural Networks, Invited talk at the International Conference on Quantum Information held at Meijo University, 4-8 Nov. 1997, Proc. of the Conference.

[9] I.V. Volovich, Models of quantum computers and decoherence problem, preprint Vito Volterra N358, 1999.

[10] I.V. Volovich, Mathematical Models of Quantum Computers and quantum decoherence problem, in Volume dedicated to V.A. Sadovnichij. Moscow State University, 1999, to be published.

[11] I.V. Volovich, Quantum Kolmogorov machine, Invited talk at the International Conference on Quantum Information held at Meijo University, 1-6 March 1999, Proc. of the Conference.

[12] I.V. Volovich, "Atomic Quantum Computer", quant-ph/9911062; Volterra preprint N. 403, 1999, Università degli Studi di Roma "Tor Vergata".

[13] I.V. Volovich: Models of quantum computers and decoherence problem. Volterra preprint N. 358, 1999, Università degli Studi di Roma "Tor Vergata".

[14] M. Ohya, I.V. Volovich: Quantum computing, NP–complete problems and chaotic dynamics. Volterra preprint N. 426, 2000, Università degli Studi di Roma "Tor Vergata".

[15] Luigi Accardi, Masanori Ohya, Ruben Sabbadini: in preparation